



STATE CORPORATION COMMISSION

REPORT ON AUDIT FOR THE PERIOD JULY 1, 2014 THROUGH JANUARY 31, 2016

Auditor of Public Accounts
Martha S. Mavredes, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

Our audit of the State Corporation Commission (Commission) for the period July 1, 2014, through January 31, 2016, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth Accounting and Reporting System and eSCC;
- matters involving internal control and its operation necessary to bring to management's attention;
- instances of noncompliance with applicable laws and regulations that are required to be reported;
- adequate corrective action with respect to one finding from the 2014 audit; and
- progress on correcting the remaining finding from the 2014 audit.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
AUDIT FINDINGS AND RECOMMENDATIONS	1-6
COMMISSION HIGHLIGHTS	7
INDEPENDENT AUDITOR'S REPORT	8-10
COMMISSION RESPONSE	11-14
COMMISSION OFFICIALS	15

AUDIT FINDINGS AND RECOMMENDATIONS

Develop, Implement, and Maintain Information Security Controls

The State Corporation Commission (Commission) does not practice consistent information security controls. For some controls, the Commission has not developed policies and procedures, while others are fully documented but not enforced. In each scenario, the Commission is not protecting their information technology (IT) environment in accordance with its own policies and procedures and the Commonwealth Information Security Standard, SEC 501-09 (Security Standard). The Security Standard requires that agencies implement minimum security controls to safeguard sensitive and mission critical data that is stored in its IT environment.

We identified the following weaknesses in the Commission's information security program that indicate a lack of appropriate documented and implemented security controls and processes. The details of which were communicated to management in the following separate recommendations:

- Improve Firewall Security Controls (Freedom of Information Act Exempt (FOIAE))
- Continue Improving the Information Security Program
- Improve Logical Access Controls (FOIAE)
- Retain Evidence of VPN Access Reviews
- Maintain and Improve Oversight of Third Party Service Providers

While the Commission's recent detection of a breach of personally identifiable information (PII) was the result of implementing new controls, the above weaknesses and absence of preventative controls may have been a contributing factor to the breach of PII for current and prior employees, as well as PII for employees' dependents and beneficiaries. Due to this incident, the Commission is paying additional expenses for credit monitoring and the services of a third-party cybersecurity firm. The Commission's lack of necessary resources to document, implement, monitor, and enforce appropriate security controls within their IT environment led to the deficiencies in it practicing appropriate separation of duties.

The Commission should dedicate resources to evaluate their current information security program to identify where the Commission is deficient in meeting the requirements of the Security Standard. The Commission should then develop, document, implement, monitor, and enforce security controls to reduce the risk of a similar security incident occurring and resolve the individual management recommendations identified above, which also are contained later in this report, as appropriate.

Improve Firewall Security Controls

The Commission does not use some required and essential controls to properly secure their perimeter firewall in accordance with their internal policies and procedures, as well as with the Security Standard.

We identified four essential control weaknesses that do not meet the Commission's security control requirements. The details of these control weaknesses were communicated to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Commission should dedicate the necessary resources to implement and improve the controls discussed in the communication marked FOIAE. Improvements to the firewall's security controls are required for compliance with the Commission's policies and procedures and the Security Standard, and also reduces risks associated with the firewall to safeguard the Commission's IT environment.

Continue Improving the Information Security Program

The Commission continues to improve their information security program in response to our fiscal year 2014 recommendation entitled "*Improve Information Security Program.*" In 2014 we reported the Commission had no documented and approved requirements to ensure that the Commission's staff, divisions, and contractors apply all the necessary controls to protect confidential and mission critical data, which are required by the Security Standard, Section 1.1.

Of the following five control areas which the Commission did not have its own approved policies and procedures in 2014, the Commission has made substantial progress in implementing two control areas (as discussed further on the next page):

- IT Systems Hardening (Sections CM-3, CM-6, SA-3-COV-2, AC-17-COV)
- Systems Interoperability (Sections CA-3, CA-3-COV)
- Malicious Code Protection (Sections SI-3, SI-3-COV)
- Data Storage and Media Protection (Sections MP-1, MP-1-COV)
- IT System and Data Backup and Restoration (Sections CP-9, CP-9-COV, CP-10)

The absence of documented and approved policies and procedures for controls increases the risk of a control failure that may cause data to be compromised, inaccurate, or lost. Additionally, without policies and procedures to govern the individual divisions' processes, the Commission increases the risk for inconsistent implementation of security controls that align with the Security Standard. Information security policies and procedures are mechanisms for the Commission to evaluate the appropriate data safeguards and allows the Commission to communicate these safeguards clearly to the staff and contractors responsible for protecting sensitive and mission critical data.

The Commission's corrective action plan indicated they would develop a detailed project plan by December 2015 that outlines details of their continued effort to align their Information Security Program with the Security Standard. While the Commission developed a detailed project plan outlining further corrective actions with a final completion date of April 2018, the milestones for detailed action are delayed due to an information security staff vacancy that was not filled until January 2016. Also, the Commission experienced a data breach incident in February 2016, further delaying the corrective action due to the reallocation of resources for investigative purposes.

The Commission has drafted and is currently implementing a Data Storage and Media Protection policy and a portion of required IT Systems Hardening policies. However, based on the delays and progress made thus far, the Commission is at risk of not meeting planned milestones for when it plans to align their full Information Security Program to the Security Standard.

The Commission should re-evaluate its corrective action plans to ensure the planned deadlines are reasonable based on the resources dedicated to the process. Additionally, the Commission should continue its efforts in improving their information security program to develop and implement the policies, procedures, and security controls as required by the Security Standard.

Improve Logical Access Controls

The Commission does not define and implement sufficient logical access controls for a mission critical system in accordance with the Commission's policies and the Security Standard.

We identified four essential control weaknesses and communicated the details to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of logical access controls.

The Commission should dedicate the necessary resources to implement and improve the controls discussed in the communication marked FOIAE to safeguard the mission critical system and ensure its confidentiality, integrity, and availability.

Retain Evidence of VPN Access Reviews

The Commission did not retain evidence that it performed annual Virtual Private Network (VPN) user account reviews. A previous audit identified that the Commission did not review VPN access for 350 users due to a lack of policies and procedures. Since that audit the Commission added VPN user account reviews to their annual access review process; however, the Commission could not provide evidence it conducted these reviews.

The Commission's Access and Account Management policy requires that the Commission perform annual user access reviews for accounts with access to sensitive systems, which includes the VPN. Additionally, the Security Standard, Section CA-6, requires agencies to update security authorizations for information systems on an annual basis.

The Commission limits its ability to hold reviewers accountable for not recognizing inappropriate VPN privileges when it does not retain evidence of who reviewed which VPN accounts for reasonableness. The Commission's inability to provide evidence of VPN reviews was caused by the Commission not creating a process for maintaining evidence of their reviews.

The Commission should continue to perform its annual reviews of the VPN user accounts in accordance with their internal policy to comply with the Security Standard and validate each user's need for access. Additionally, the Commission should develop and implement a process for maintaining the necessary evidence of each review.

Maintain and Improve Oversight of Third Party Service Providers

The Commission does not maintain sufficient oversight over certain third party service providers (Providers) in order to gain assurance over outsourced operations. Specifically, the Commission does not gain assurance over four IT Providers out of a total of ten Providers that the Commission utilizes for outsourced fiscal and IT processes.

The Security Standard, Section 1.1, states that agency heads remain accountable for maintaining compliance with the Security Standard for IT equipment, systems, and services procured from Providers, and must enforce the compliance requirements through documented agreements and oversight of the services provided. Additionally, the Commonwealth Accounting Policies and Procedures Manual Topic 10305 requires agencies to have adequate interactions with Providers to understand each Provider's internal control environment and maintain oversight over their Providers to gain assurance over outsourced operations. The Commission can obtain assurance in several forms including, but not limited to, service organization control (SOC) reports, independent security audit reports, and/or on-site reviews of the Provider's internal control structure as needed.

Without maintaining oversight, the Commission cannot gain assurance and validate that the Provider's internal control structure is sufficient to protect the Commonwealth's assets and data. While the Chief Internal Auditor reviewed SOC reports for six Providers of outsourced fiscal processes, the evaluation did not include the four Providers delivering IT services the Commission outsourced. This is because the Commission does not have policies and procedures for reviewing and assessing the effectiveness of controls for all Providers. Furthermore, the Commission did not identify IT Providers as being an attribute of fiscal processes.

The Commission should develop and implement formal policies and procedures to maintain appropriate oversight and gain assurance from Providers. This process should include a framework for identifying all of the Commission's Providers and applicable sub-service organizations, and ensuring contracts with Providers require documented independent assurances over controls be provided to the Commission on a periodic basis. Additionally, the Commission should ensure the process for evaluating the forms of assurance includes documenting managements final decisions and action items, as needed.

Disable System Access in a Timely Manner

The Commission is not consistently disabling system access in a timely manner for employees no longer needing access. Of the ten terminated employees tested, the Commission did not disable access in a timely manner in eight cases (80 percent). To comply with the Security Standard, Section AC-2 COV, 2.e - f, the Commission's Access and Account Management policy requires the Commission to disable access within 24 hours of an employee no longer needing access.

The eight exceptions for not disabling an employee's access in a timely manner are as follows:

- In four cases, access was not disabled timely from the active directory and the Commission's internal systems.
- In two cases, access was not disabled timely from the active directory, but was properly disabled from the Commission's internal systems.
- In two cases, access was properly disabled from the active directory, but was not disabled timely from the Commission's internal systems.

In five cases, access was not disabled timely because individuals completing the forms that requested the access to be disabled entered the wrong date as the effective date. For example, an employee may depart their position and then take three weeks of leave before they are officially terminated from the Commission. In this example, the employee no longer needs access when they stop working and should not retain access for the remaining three weeks. Additionally, in three cases, access was not disabled timely because divisions did not submit the System Access Request forms to the Office of Information Security timely or the request was not completed timely. While risks to the Commission's data is limited if access to the active directory is disabled timely, terminated employees who retain access to information systems and the active directory increase the risk of alterations of data and/or inappropriate transactions. For 40 percent of the employees tested, access was not disabled timely for both an information system and the active directory.

The Commission should clarify the effective date that should be used to initiate the disabling of account access and update the Access and Account Management policy as necessary. In addition, divisions and the Office of Information Security should process Systems Access Forms timely.

Status of Prior Finding: Follow Procurement Rules and Best Practices

Our fiscal year 2014 report included an update on 2012 findings that management was in progress of resolving. As a part of this year's audit, we followed up with management on the status of the remaining finding not resolved, entitled *Follow Procurement Rules and Best Practices*. During the 2012 audit, we found that the Commission did not always follow, consider, or document compliance with procurement rules and regulations when making purchases. We recommended that the Commission work with the Department of General Services (General Services) and the Attorney General's Office to clarify what procurement rules and regulations apply to them as an independent department of government, and to review the current policies and procedures and

change them as needed to agree with this clarified understanding. It was also recommended that the Commission review its current contracts to ensure that they were properly procured.

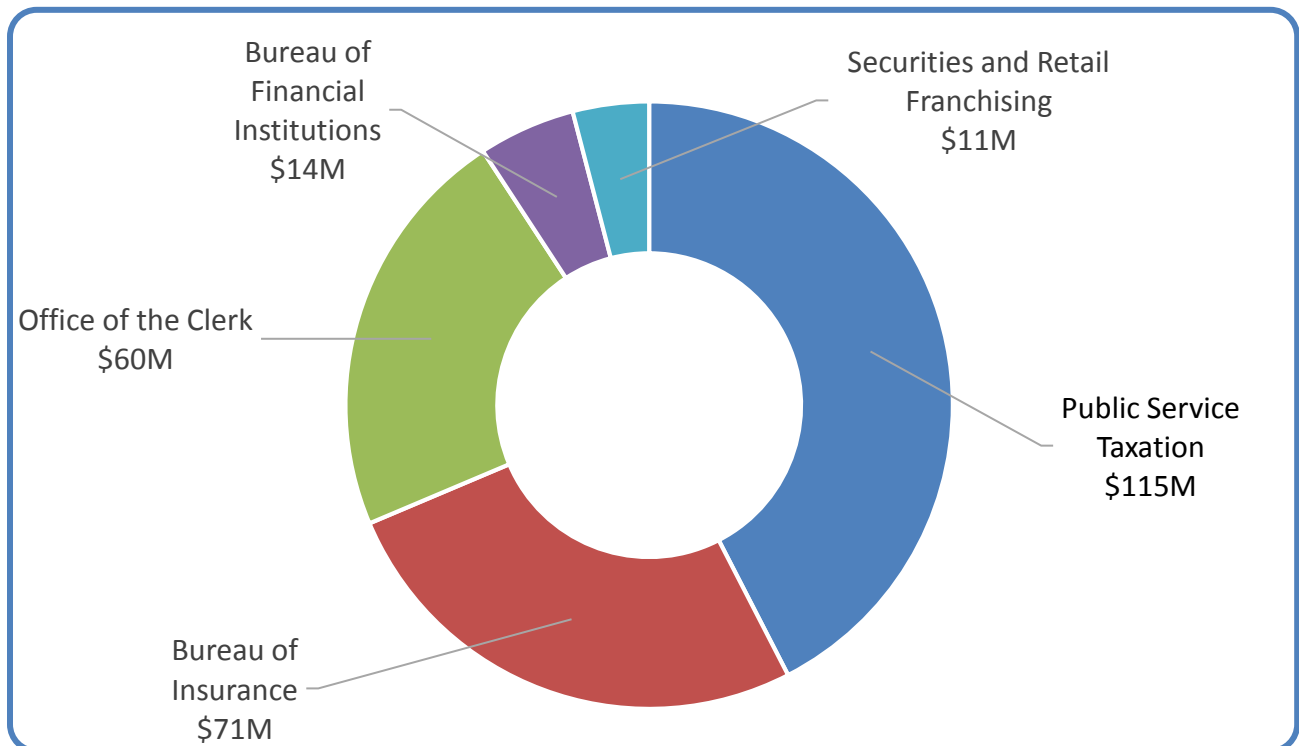
Since our 2014 audit, the Commission has met with the Attorney General's Office and General Services. The Commission's management has made a commitment to comply with all applicable provisions of the Virginia Public Procurement Act. In addition, management has stated it will follow regulations promulgated by General Services pursuant to §2.2-1111 of the Code of Virginia, and central purchasing requirements and policies contained in each, as a general operations policy; however, should a specific issue arise that poses operational or legal difficulties or conflicts, the Commission will consult with the Attorney General for advice and counsel. To implement these commitments, management has begun the process of reviewing the current policies and procedures manual and have met to discuss approaches to and the structure for proposed revisions to the existing procurement manual; however no revisions have occurred as of July 8, 2016.

COMMISSION HIGHLIGHTS

The Commission is an independent state agency established by the Constitution of Virginia. The Commission is directed by three Commissioners, elected by the General Assembly for six-year terms. Regulatory divisions have authority over utilities, insurance, state-chartered financial institutions, securities, retail franchising and railroads. The Commission also serves as the Commonwealth's central filing office for corporations, limited partnerships, limited liability companies, business trusts and Uniform Commercial Code filings. Non-regulatory divisions provide administrative and legal support to the regulatory divisions.

The Commission's regulatory divisions collect revenues for the General Fund, other special revenues funds, localities and other state agencies. In total, the regulatory divisions collect around \$271 million each year, as seen in the table below. To collect these funds and fulfill its mission, the Commission uses various information systems. For some systems, the Commission outsourced the maintenance and control to service providers. While the systems are outsourced, the Commission is responsible for maintaining oversight of the service providers and ensuring that the Commonwealth's Security Standards are met to protect the Commonwealth's sensitive information.

**Revenue Collected by Regulatory Division
Fiscal Year 2015**



Source: Commonwealth Accounting and Reporting System



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

July 12, 2016

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations of the **State Corporation Commission (Commission)** for period July 1, 2014, through January 31, 2016. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objectives were to evaluate the accuracy of recorded financial transactions in the Commonwealth Accounting and Reporting System and eSCC, review the adequacy of the Commission's internal controls, test compliance with applicable laws, regulations, contracts, and grant agreements, and review corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

The Commission's management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances.

Revenues, including revenue refunds
Expenses (payroll and non-payroll)
Statement of Economic Interests
Information System Security, including access controls

Our audit excluded an evaluation of the Commission's procurement cycle because the Commission had not revised their procurement manual since our last audit. On August 14, 2015, we issued a special report entitled, *A Special Review of Procurement of Commission 2.0 at the State Corporation Commission*, which can be found at www.apa.virginia.gov.

We performed audit tests to determine whether the Commission's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of the Commission's operations. We tested transactions and performed analytical procedures, including budgetary and trend analyses.

Conclusions

We found that the Commission properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System and eSCC. The Commission records its financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America. The financial information presented in this report came directly from the Commonwealth Accounting and Reporting System.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts and grant agreements that require management's attention and corrective action. These matters are described in the section entitled "Audit Findings and Recommendations."

The Commission has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this letter. Progress on other prior year findings is discussed in the section titled "Audit Findings and Recommendations."

Exit Conference and Report Distribution

We discussed this report with management on September 14, 2016. Management's response to the findings identified in our audit is included in the section titled "Commission Response." We did not audit management's response and, accordingly, we express no opinion on it.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

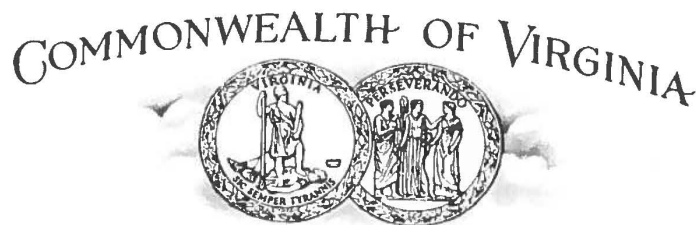
AUDITOR OF PUBLIC ACCOUNTS

GDS/clj

MARK C. CHRISTIE
COMMISSIONER

JAMES C. DIMITRI
COMMISSIONER

JUDITH WILLIAMS JAGDMANN
COMMISSIONER



JOEL H. PECK
CLERK OF THE COMMISSION
P.O. BOX 1197
RICHMOND, VIRGINIA 23218-1197

STATE CORPORATION COMMISSION

September 14, 2016

Ms. Martha S. Mavredes
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

The State Corporation Commission (Commission) appreciates the time and effort your staff devoted to the Auditor of Public Accounts' (APA) review of the Commission's financial records and operations for the period July 1, 2014 through January 31, 2016 (Report). We welcome your comments indicating that the Commission properly recorded and reported all transactions in all material respects in the relevant financial management systems; took adequate corrective action with respect to one finding from the 2014 audit; and made progress correcting the remaining finding from the 2014 audit.

The Commission is aggressively pursuing corrective actions on the matters of internal controls and instances of noncompliance cited in the Report, all of which are related to information security and information technology. The following actions have either been taken or will be initiated.

Develop, Implement, and Maintain Information Security Controls

The Commission's internal resources and the services of a major information technology (IT) vendor continuously monitor and scan systems and networks to identify potential threats and suspicious activity. The Commission is in the process of upgrading to a new Intrusion Prevention and Detection system with new SIEM technology. This enhanced system will provide greater visibility and control against attacks in the Commission's environment.

During the audit period, a Vulnerability Management Program was implemented that decreased the Commission's server vulnerabilities by 67 percent and workstation vulnerabilities by 78 percent. The Commission uses a new server patch management tool to meet internal requirements, and weekly IT meetings focus on patch management and the ongoing effort to reduce vulnerabilities. There is now a higher level of awareness and understanding of vulnerabilities in the infrastructure and the inherent risk to the Commission's environment.

A Health Check process was recently implemented to ensure that all systems are scanned and that tools protecting the environment remain operational. This process requires alerts to be investigated on the day discovered. As noted in your Report, these new controls were largely responsible for the detection of the data breach. Upon identification and investigation of the suspicious activity, various steps were initiated to ascertain the extent of the incident and begin

mitigation. The contractor responsible for the data breach was terminated, and the Commission worked with the Federal Bureau of Investigation and appropriate state agencies, including the Virginia Information Technologies Agency, the Office of the Attorney General, the Virginia State Police and the Division of Capitol Police. Although there were no specific indications that personal information was acquired, out of an abundance of caution and in compliance with state law, those individuals whose information was associated with the breach were notified of the situation and provided information on measures they should pursue to protect themselves.

During the audit period, a new Information Security Policy and a new Usage Standard related to individual use of information and IT resources were created. All Commission employees and contractors were trained, and the same training is now required for all new hires. System Hardening Standards for server and workstation environments were documented and implemented to comply with the requirements stipulated in SEC501-09, the Commonwealth's Information Security Standard.

The implementation of these "technical controls" has significantly improved the Commission's security posture and aided in the robust monitoring of activity in the Commission's environment.

Improve Firewall Security Controls

The Commission's Office of Information Security worked with application owners to document all dataflows for traffic traversing the Commission's firewall. The documentation includes all ports and protocols being used, and only appropriate and approved traffic can flow between network zones. In April 2016 a new project manager was hired to implement the technology and process improvements needed to further strengthen the Commission's IT security program.

An example of a recent process improvement is that all firewall changes now require pre-approval by the security team prior to review by the Change Control Board. This change provides a system of checks and balances to eliminate the ability of any one person to make changes. New controls are being assessed to determine if all appropriate changes are going through this new process.

Continue Improving the Information Security Program

In 2015 the Commission's Information Security Officer (ISO) completed a Capability Maturity Model assessment of the Commission's Information Security Program. This assessment identified areas for improvement and established specific goals for 2015 through 2017, prioritizing missing controls that posed the greatest risk. For example, OIS implemented controls concerning elevated administrator access. Further, specific actions are underway that will substantially improve and fortify authentication for remote access. These steps alone will significantly strengthen the Commission's security posture.

In January 2016 the Commission hired a new IT security analyst with responsibility for improving the policies and procedures of the Commission's risk management program. A new risk management framework was created and tested with applications, and risk assessments are being conducted with the Commission's business areas. There is a schedule for the creation of a new set of standards to be added to the policy framework, the first of which is directly applicable to those with elevated access in the Commission's environment to ensure that they understand their responsibilities

and accountability when managing the infrastructure. Many of the lessons learned from the security breach are part of these standards, and the system administrators will be trained on the new standards. Additionally, there is now a template to be used when reviewing all proposed new technology implementations to ensure compliance with SEC501-09. Security reviews are now conducted earlier in the system life cycle, and appropriate controls are applied throughout. Finally, this new security analyst works with the Commission's internal audit team to reassess corrective action plans to ensure that a reasonable approach is in place to meet the requirements needed to implement new policies.

To bring about greater transparency and accountability over technology management, the Commission recently restructured the Information Technology Division. The new structure, in part, further emphasizes the importance of information security by including the Manager of Information Security as a member of a newly created IT executive team. The team is comprised of the four senior IT managers, and each now reports directly to the Chief Administrative Officer (CAO).

Improve Logical Access Controls

The Commission annually reviews, documents and validates the access privileges assigned to users of information systems. The Commission will ensure that authorization documentation is maintained for users of critical systems and that privileged users are included in the annual review. The reports used for performing the annual reviews of users' access privileges contain statements indicating that the data owners or authorized representatives of the information systems certify that the access privileges shown are the minimum required for the users to perform their jobs and that there is a continued need for the access. The Commission asserts that this review process, in addition to the other internal procedures used for granting logical access to information systems, is a sufficient internal control for the Commission's operating environment and will bring the Commission into compliance with SEC501-09. Every effort will be made to ensure that the internal procedures are followed when submitting user access changes.

Retain Evidence of VPN Access Reviews

A new process has been implemented to retain all access review reports in the OIS SharePoint site. Scheduled reviews of all access eligibility will be conducted, and the reports will be saved in the SharePoint library. This approach will improve the process for maintaining copies of the review reports that were previously retained in hard copy form.

Maintain and Improve Oversight of Third-Party Service Providers

The Commission intends to develop a standard to address the oversight of all third-party service providers. In the past, and as recognized by the APA auditor, the Commission provided oversight of the third-party service providers whose services impacted the Commission's fiscal processes. For the third-party service providers whose services impact the Commission's IT processes, the Commission's Office of Internal Audit has requested, and for some providers already obtained and reviewed, the Service Organization Controls Reports (SOC Reports) to identify any areas of concern. The Chief Internal Auditor (CIA) will notify the CAO of those providers whose SOC Reports have issues that could potentially impact the Commission's fiscal or IT processes.

Disable System Access in a Timely Manner

The CIA performed research on the exceptions identified in the draft audit report. Based upon that research, the Commission's practices and procedures will be revised to ensure that a terminated employee's system access is disabled in a timely manner.

In closing, thank you for the opportunity to review and comment on the APA's draft audit report. The Commission recognizes its responsibility to protect its information, network, and systems from unauthorized access and has been working diligently to identify and implement necessary improvements. We look forward to working with the APA to achieve that shared goal.

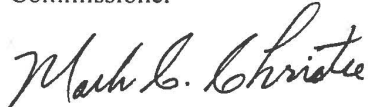
Sincerely,



James C. Dimitri
Chairman



Judith Williams Jagdmann
Commissioner



Mark C. Christie
Commissioner

STATE CORPORATION COMMISSION

As of January 31, 2016

Commissioners

James C. Dimitri
Chairman

Mark C. Christie

Judith Williams Jagdmann